ELECTRONIC FRONTIER FOUNDATION

Government Hacking and Subversion of Digital Security

Too often, the policies and practices of law enforcement and intelligence agencies can be disastrous for security.

Attempts to weaken encryption through law, policy, or informal pressure can make technology devices less secure for everyone. Government agents may infiltrate, copy, delete, or damage data during digital investigations. The government may even actively create and disseminate malware that can damage computers. We've seen these dangerous techniques employed both in the United States and in countries around the world, and they inevitably have the same consequence: we are less secure.

Government attacks on security come in many disguises, including:

- **State-sponsored malware.** The government will design and deploy malicious code that infects computers, a technique often employed by authoritarian governments to uncover or silence dissent. Read about state-sponsored malware.
- **Stockpiling or exploiting vulnerabilities.** The government may find or purchase details of security vulnerabilities and then use them for investigative or "offensive" purposes. The U.S. government has created a policy, known as the **Vulnerabilities Equities Process (VEP)**, to decide whether to disclose information about security vulnerabilities or instead withhold this information for its own purposes**.** This process is opaque, leaving the public in the dark about how frequently security vulnerabilities are left unaddressed. Although the government says the process is biased in favor of disclosure, there is no requirement in the VEP to tell technology makers about their security flaws.
- **Promoting crypto backdoors.** Whether through legislation, litigation, or unofficial pressure, government attempts to undermine crypto, defeat

security features, obtain "keys" to unlock encrypted data, or insert vulnerabilities into software make us all less secure.
- **Malicious hacking.** Whether sanctioned by a court or not, the government may actively break into computers remotely. Agents may access, copy, delete, or even create data in order to suit their needs. Too often, these practices are shrouded in secrecy with inadequate oversight by the judicial system, beginning with opaque and overbroad warrants authorizing installation of malware, all the way up to refusals to share details of the malware with defendants as part of a fair trial.

These tools can have dire consequences for the security and privacy of users who have done nothing wrong and are not even connected to an investigation. In other cases, these tools are disproportionate to the threat, wreaking havoc on users' computers when less invasive techniques would have been appropriate.

In balancing the need for strong security against the potential benefit of hacking and other anti-security techniques, the government—including the courts—must carefully consider the costs to society. The public needs to be able to access secure digital tools. And as a society, we have an interest in protecting innocent users from the collateral effects of intrusive surveillance, whether by law enforcement and intelligence agencies.

Above all, the government must be accountable to the people, and that means promoting strong crypto and security.